WHAT IS CLAIMED IS:

1. A method for communication over a network that allows for the authentication of individuals and control of information comprising:

initiating a communication from a first user via a first client machine to a second user via a second client machine utilizing an augmented email address that functions appropriately only between the first user and the second user, wherein augmented email address contains a public encryption key;

receiving at the second client machine the communication utilizing the augmented email address and validating that it was received from the first user via the first client machine.

2. The method as recited in claim 1, wherein the public encryption key is self-validating because the email address functions appropriately only between the first user and the second user.

3. The method as recited in claim 1, wherein the communication between the first and second users is encrypted utilizing the public encryption key.

4. A method for selling a product over a network that allows for the authentication of individuals and control of information comprising:

establishing a first identity by an individual with a central server;

establishing a second identity by a product supplier with said central server;

contacting by said individual to said product supplier resulting in a communication that takes place over said network, wherein said product supplier recognizes said first identity, wherein said communication results in a sale of a product;

sending said product to said individual;

notifying said central server that said product was sent; and

releasing a payment authorized by said central server for said product to said product supplier on behalf of said individual.

5. The method as recited in claim 4, wherein establishing said second identity occurs before establishing said first identity.

6. The method as recited in claim 4, wherein said central server is at least two separate machines in communication over said network

7. A method for distributing products via a network that allows for the authentication of individuals and control of information comprising:

establishing a first identity for a first dealer with a discovery machine linked to said network;

providing a dealer website on said network wherein said dealer website corresponds to said first dealer in a first geographic area;

capturing a customer sale for a product on said dealer website for a customer, wherein said customer resides in a second geographic area;

establishing a second identity for a second dealer with at least one of said discovery machine linked to said network and a second discovery machine linked to said network, wherein said second dealer is located in said second geographic area;

establishing a direct connection between said first and said second dealer on said network;

checking for said product in an inventory of a said second dealer via said direct connection;

delivering said product to said customer if said product is present in said inventory;

reporting said customer sale to a central server on said network from said first dealer; and

providing a sales credit from said central server to both said first and second dealers.

8. The method as recited in claims 7, wherein said discovery machine and said second discovery machine are in communication over said network.

9. The method as recited in claims 7, wherein at least one of said discovery machine and said second discovery machine are said central server.

10. Method of creating a managed information communication agreement (MICA), the method comprising:

generating a new public/private key pair;

converting the public key of the public/private key pair into a string to create a key field of the MICA;

selecting the desired value for a credential field of the MICA and retrieve the value of each item that is desired for inclusion in the credential field;

computing a hash of information drawn from the credential field and the key field;

encrypting the computed hash using the private key of the public/private key pair;

converting the encrypted computed hash into a string to produce a validation field; and

assembling the MICA by concatenating the key field, the validation field, and the credential field.

11. The method of creating a MICA of claim 10, wherein the new public/private key pair generated is limited in usefulness to a single relationship among a predetermined set of plural user identities.

12. The method of creating a MICA of claim 10, wherein the credential field includes an email address of an intended recipient.

13. The method of creating a MICA of claim 10, wherein the credential field includes credential information selected from the group consisting of: IP address of a mail server used by an intended recipient and custom mail attributes.

14. A method for validation of a managed information communication agreement (MICA) associated with an electronic item, the method comprising:

confirming that the electronic item received contains credentials specified by a credential field of the MICA;

computing a hash based on information from the electronic item, including values of the credential field and a key field of the MICA;

decrypting a validation field of the MICA using a private key and a public key of the MICA;

encrypting the computed hash using the private key of the MICA;

converting the encrypted computed hash into a string;

comparing the string to the validation field; and

validating to an owner of the MICA relationship that the electronic item represents a legitimate use of the MICA if the values of the string and the validation field are the same.

15. A computer program product for enabling a computer to create a managed information communication agreement (MICA) comprising:

software instructions for enabling the computer to perform predetermined operations, and

a computer readable medium bearing the software instructions;

the predetermined operations including the steps of:

generating a new public/private key pair;

converting the public key of the public/private key pair into a string to create a key field of the MICA;

selecting the desired value for a credential field of the MICA and retrieve the value of each item that is desired for inclusion in the credential field;

computing a hash of information drawn from the credential field and the key field;

encrypting the computed hash using the private key of the public/private key pair;

converting the encrypted computed hash into a string to produce a validation field; and

assembling the MICA by concatenating the key field, the validation field, and the credential field.

16. The computer program product of claim 15, wherein the credential field includes an email address of an intended recipient.

17. The computer program product of claim 15, wherein the credential field includes credential information selected from the group consisting of: IP address of a mail server used by an intended recipient and custom mail attributes.

18. A computer program product for enabling a computer to validate a managed information communication agreement (MICA) associated with an electronic item comprising:

software instructions for enabling the computer to perform predetermined operations, and

a computer readable medium bearing the software instructions;

the predetermined operations including the steps of:

confirming that the electronic item received contains credentials specified by a credential field of the MICA;

computing a hash based on information from the electronic item, including values of the credential field and a key field of the MICA;

decrypting a validation field of the MICA using a private key and a public key of the MICA;

encrypting the computed hash using the private key of the MICA;

converting the encrypted computed hash into a string;

comparing the string to the validation field; and

validating to an owner of the MICA relationship that the electronic item represents a legitimate use of the MICA if the values of the string and the validation field are the same.

19. A method for communication over a network that allows for the authentication of individuals and control of information comprising:

initiating a communication from a first user via a first client machine to a predetermined group of users via respective client machines of the group of users utilizing an managed information communication agreement (MICA) that functions appropriately only between the first user and the predetermined group of users;

receiving at the respective client machines of the group of users the communication utilizing the MICA and validating that it was received from the first user via the first client machine.

20. A method for communication over a network that allows for the authentication of individuals of a group and control of information comprising:

registering with a discovery machine a group of plural users, wherein each of the plural users maintains a respective client machine, wherein the respective client machines of the plural users and the discovery machine are coupled to a network;

initiating a communication from one of the plural users via that user's respective client machine to the rest of the group of plural users via their respective client machines through said discovery machine;

determining that the rest of the group of plural users will accept the communication;

establishing a direct link between the respective client machines of the plural users; and

delivering said communication.